



Manual de usuario en materia de protecci· n de datos de car§cter personal de la entidad

Universidad de Almería.

ADAPTADO AL REAL DECRETO 1720/2007

Mayo de 2011

Índice

1. Introducci· n ... 1
2. Glosario de t®rminos b§sicos ... 3
3. Niveles de seguridad de los datos ... 6
4. Funciones y obligaciones de los usuarios ... 8
5. Gesti· n de incidencias ... 14
5.1. Procedimiento para la gesti· n de incidencias relativas a ficheros automatizados ... 15
5.2. Procedimiento para la gesti· n de incidencias relativas a ficheros no automatizados ... 15
6. Ejercicio de derechos ... 17
6.1. Introducci· n ... 17
6.2. Disposiciones comunes ... 17
6.2.1. Car§cter personal²simo (Art²culo 23 RDLOPD) ... 17
6.2.2. Acreditaci· n de la personalidad o representaci· n (Art²culo. 23 RDLOPD) ... 17
6.2.3. Condiciones generales para el ejercicio de los derechos de acceso (Art²culo 24 RDLOPD) ... 18
6.2.4. Inicio: solicitud ... 18
6.2.5. Contestaci· n ... 18
6.2.6. Ejercicio de derechos ante el encargado del tratamiento ... 19
6.3. Derecho de acceso ... 19
6.3.1. Concepto (Art²culo 27 RDLOPD) ... 19
6.3.2. Forma de acceso (Art²culo 28 RDLOPD) ... 20
6.3.3. Contestaci· n ... 20
6.3.3.1. Otorgamiento del acceso (Art²culo 29 RDLOPD) ... 21
6.3.3.2. Denegaci· n del acceso. (Art²culo 30 RDLOPD) ... 21
6.4. Derechos de rectificaci· n y cancelaci· n ... 21
6.4.1. Concepto (Art²culo 31 RDLOPD) ... 22
6.4.2. Solicitud (Art²culo 32 RDLOPD. Ejercicio de los derechos de rectificaci· n y cancelaci· n) ... 22
6.4.3. Contestaci· n (Art²culo 32. Ejercicio de los derechos de rectificaci· n y Cancelaci· n) ... 22
6.4.4. Comunicaci· n al cesionario ... 22
6.4.5. Denegaci· n (Art²culo 33. Denegaci· n de los derechos de rectificaci· n y cancelaci· n) ... 23
6.5. Derecho de oposici· n ... 23
6.5.1. Concepto (Art²culo 34. Derecho de oposici· n) ... 23
6.5.2. Solicitud (Art²culo 35. Ejercicio del derecho de oposici· n) ... 24
6.5.3. Contestaci· n (Art²culo 35. Ejercicio del derecho de oposici· n) ... 24
6.5.4. Exclusi· n (Art²culo 35. Ejercicio del derecho de oposici· n) ... 24
6.6. Derecho de oposici· n a las decisiones basadas ¼nicamente en trat. auto. ... 24
6.6.1. Concepto ... 24
6.6.2. Excepciones ... 24
6.7. Procedimiento establecido por la organizaci· n ... 25
7. Procedimiento para el uso del correo electr· nico ... 27
8. Procedimiento para los env²os telem§ticos ... 28
9. Procedimiento de registro de entrada de soportes ... 30
10. Procedimiento de registro de salida de soportes ... 31
11. Procedimiento de desechado y reutilizaci· n de soportes automatizados ... 33

12. Procedimiento de desechado y reutilizaci· n de soportes no automatizados 34
13. Procedimiento de custodia de soportes no automatizados 36
14. Procedimiento de archivo de ficheros no automatizados 37
15. Procedimiento de restricci· n de acceso a ficheros no automatizados 38
16. Procedimiento de copia y reproducci· n de documentos 39
17. Procedimiento de traslado de documentaci· n 40
18. Responsables de seguridad 41
ANEXO A. Modelo de notificaci· n de incidencias del nivel b§sico 42
ANEXO B. Modelo de notificaci· n de incidencias del nivel medio / alto 44
ANEXO C. Modelo de derecho de acceso 46
ANEXO D. Modelo de derecho de rectificaci· n 48
ANEXO E. Modelo de derecho de cancelaci· n 50
ANEXO F. Modelo de derecho de oposici· n 52
ANEXO G. Modelo de derecho de impugnaci· n de valores 54
ANEXO H. Modelo de derecho de acceso (videovigilancia) 56
ANEXO I. Modelo de derecho de cancelaci· n (videovigilancia) 58

1. Introducción

La protecci· n de los datos de car§cter personal de los ciudadanos ha sido regulada por el legislador espa¶ol mediante la L.O. 15/1999 (LOPD) y una serie de normas que la desarrollan y complementan, que establecen toda una serie de medidas de obligado cumplimiento para aquellas entidades que, en el ejercicio de su actividad, sometan a tratamiento este tipo de datos de car§cter personal.

El RD 1720/2007, Reglamento de desarrollo de la LOPD, o RDLOPD), desarrolla los principios y obligaciones dispuestos en la LOPD.

La LOPD y el RDLOPD, cuyo objeto principal lo constituye la salvaguarda del derecho al honor, la intimidad personal, y la propia imagen de las personas f²sicas, atribuyen determinadas funciones y obligaciones a todas aquellas personas que intervienen en el tratamiento de los ficheros donde se almacenan los datos de car§cter personal.

La Ley impone sanciones econ· micas muy elevadas a las organizaciones privadas (sanciones que pueden llegar - s· lo por una infracci· n - hasta los 600.000 euros) y sanciones no econ· micas pero si de otra ²ndole (publicidad de la sanci· n, inmovilizaci· n temporal del fichero, etc...) a las organizaciones p¼blicas.

Es, por tanto, objeto de este manual el detallar las funciones y obligaciones que, como usuario de los ficheros con datos de car§cter personal de la entidad, le corresponde conocer y respetar.

Entre los derechos que la Ley otorga a los interesados est§n los de acceder, rectificar, cancelar u oponerse al tratamiento de sus datos.

Hay que destacar, que ®ste, es uno de los puntos m§s importantes de la legislaci· n relativa a la Protecci· n de Datos de Car§cter Personal, dado que un mal conocimiento o mala gesti· n del procedimiento de ejercicio de derechos suele ser la antesala de un posible procedimiento sancionador.

Debido a esto es importante que en las organizaciones existan unos usuarios (a los que denominamos usuarios de atenci· n) que son los encargados de recoger estas

peticiones (normalmente en las empresa los servicios de atenci· n al cliente, o en las organizaciones p¼blicas los servicios de atenci· n al ciudadano o quienes se hallen en los registros de entrada) y otras personas (los responsables de seguridad) encargados de atender (contestar) dichas peticiones.

Es, por tanto, objeto de este manual el detallar las funciones y obligaciones que, como usuario de atenci· n de la organizaci· n le corresponde conocer y respetar.

2. Glosario de términos básicos

DATOS DE CARĆCTER PERSONAL: cualquier informaci· n concerniente a personas f²sicas identificadas o identificables.
Es decir, cualquier dato que podamos relacionar con personas f²sicas. En el §mbito de las empresas esas personas ser§n normalmente potenciales clientes, clientes, proveedores, trabajadores de la empresa, terceros o personas de contacto. En algunos §mbitos concretos de actividad puede que los datos se refieran a otras personas como pacientes, asociados ... o por ejemplo en el §mbito p¼blico dichos afectados son los ciudadanos, contribuyentes etc., adem§s de algunos afectados comunes al §mbito privado: por ejemplo los empleados, proveedores, contactos, etc... T®ngase en cuenta que no s· lo se refiere a personas identificadas (cuando tengamos su nombre) sino tambi®n cuando esas personas sean razonablemente identificables por ejemplo a trav®s de un identificador: por ejemplo n¼mero de colegiado, DNI, IP, correo electr· nico etc...
AFECTADO O INTERESADO: persona f²sica titular de los datos.
Es la persona cuyos datos se tratan, es decir: el cliente, paciente, ciudadano, empleado, proveedor, contacto, etc...
TRATAMIENTO DE DATOS: operaciones y procedimientos t®cnicos de car§cter automatizado o no, que permitan la recogida, grabaci· n, conservaci· n, elaboraci· n, modificaci· n, bloqueo y cancelaci· n, as² como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
T®ngase en cuenta que a tenor de la definici· n de tratamiento que da la Ley cualquier operaci· n que se haga con ellos: grabarlos, modificarlos, conservarlos, enviarlos, etc... constituir§ tratamiento.
FICHERO: todo conjunto organizado de datos de car§cter personal, cualquiera que fuere la forma o modalidad de su creaci· n, almacenamiento, organizaci· n y acceso. Es decir, cualquier dato que tengamos sobre personas f²sicas en cualquier tipo de soporte, tanto papel como a nivel inform§tico.

El concepto de fichero no se corresponde necesariamente con una base de datos, sino que siempre que exista un conjunto de datos que est®n organizados mediante alg¼n criterio, nos encontraremos ante la existencia de un fichero. Obviamente una aplicaci· n inform§tica de n· minas constituye un ejemplo de fichero, pero tambi®n lo puede constituir una tabla de datos en Word, sin olvidar que tambi®n es aplicable este concepto a los datos no automatizados: por ejemplo un archivo A-Z.

RESPONSABLE DEL FICHERO O TRATAMIENTO: Persona f²sica o jur²dica, de naturaleza p¼blica o privada, u · rgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

El responsable del fichero normalmente coincidir§ con la organizaci· n: la empresa, asociaci· n, instituci· n, empresarios individual, profesional, etc... y es a quien se le imponen la mayor²a de las obligaciones en protecci· n de datos siendo, por tanto, normalmente el responsable de las sanciones que - en su caso - se impongan. Ello sin perjuicio de que el responsable del fichero pueda nombrar una persona f²sica que le represente.

ENCARGADO DEL TRATAMIENTO: la persona f²sica o jur²dica, autoridad p¼blica, servicio o cualquier otro organismo que, s· lo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

El encargado del tratamiento es un tercero (normalmente una empresa pero no necesariamente) que le presta un servicio al responsable del fichero y que para ello requiere acceder a datos del responsable. Ejemplos t²picos de encargados lo son la asesor²a laboral, contable o fiscal (que acceden a los datos de empleados, clientes o proveedores de su cliente para asesorarle), empresas de mantenimiento de hardware o software, etc... El servicio que presta el encargado no tiene porqu® ser remunerado. La relaci· n entre el responsable y el encargado se debe regular mediante un contrato cuyo contenido establece el art²culo 12 de la LOPD.

USUARIOS: sujeto o proceso autorizado a acceder a datos o recursos.

Normalmente un usuario ser§ una persona que accede a datos de la organizaci· n. El usuario podr§ tener diferentes perfiles de acceso y ser un usuario interno o externo (un usuario de otra organizaci· n que accede a nuestro sistema para prestar un servicio, por ejemplo mantenimiento inform§tico).

RESPONSABLE DE SEGURIDAD: El responsable del fichero designar§ uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ning¼n caso esta designaci· n supone una delegaci· n de la responsabilidad que corresponde al responsable del fichero.
El responsable de seguridad puede ser uno o varios y son los encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ning¼n caso esta designaci· n supone una delegaci· n de la responsabilidad que corresponde al responsable del fichero, que es a quien en primera instancia se le pueden imponer en su caso las sanciones que contempla la Ley. Ello es sin perjuicio de que el responsable de seguridad si no cumple con sus obligaciones pueda tener responsabilidad laboral o disciplinaria.
CONSENTIMIENTO: Toda manifestaci· n de voluntad, libre, inequ²voca, espec²fica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
T®ngase en cuenta que el consentimiento es el eje vertebral de la protecci· n de datos y ello exige que como regla general no se puedan tratar datos de nadie sin se consentimiento, sin perjuicio de que en ocasiones esta obligaci· n est§ exenta. Por ejemplo: cuando los datos se traten en el marco de la relaci· n negocial, laboral o administrativa, cuando exista una Ley que disponga lo contrario, etc...
COMUNICACIč N DE DATOS: Toda revelaci· n de datos realizada a una persona distinta del interesado.
La cesi· n de datos debe estar, salvo excepciones, necesariamente consentida por el interesado. Por ello, es importante no comunicar datos de car§cter personal a otras personas f²sicas o jur²dicas, salvo que se disponga del consentimiento de dicha persona o se est®ante alguna de las excepciones previstas por la Ley.

3. Niveles de seguridad de los datos

Las medidas de seguridad que dispone el RDLOPD se dividen en tres niveles, seg¼n la sensibilidad de los datos que se contienen en los ficheros: nivel b§sico, medio y alto. Las medidas se aplican de modo acumulativo.

Tenga en cuenta que deber§n cumplirse - como m²nimo - las medidas correspondientes al nivel del fichero. Sin embargo, el Responsable de Seguridad podr§ implementar medidas de nivel superior cuando as² considere oportuno.

NIVEL	DESCRIPCIč N
B§sico	- Todos
Medio	- Los relativos a la comisi· n de infracciones administrativas o penales. - Los relativos al art. 29 LOPD (ficheros de solvencia patrimonial y cr®dito). - Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. - Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. - Aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. - Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestaci· n de servicios financieros. - Aquellos que contengan un conjunto de datos de car§cter personal que ofrezcan una definici· n de las caracter²sticas o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

Alto	- Los que se refieran a datos de ideolog²a, afiliaci· n sindical, religi· n, creencias, origen racial, salud o vida sexual. - Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. - Aquellos que contengan datos derivados de actos de violencia de g®nero.
EXCEPCIONES	- A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electr· nicas disponibles al p¼blico o exploten redes p¼blicas de comunicaciones electr· nicas respecto a los datos de tr§fico y a los datos de localizaci· n, se aplicar§n, adem§s de las medidas de seguridad de nivel b§sico y medio, la medida de seguridad de nivel alto contenida en el art²culo 103 de este reglamento (registro de accesos). - En caso de ficheros o tratamientos de datos de ideolog²a, afiliaci· n sindical, religi· n, creencias, origen racial, salud o vida sexual bastar§ la implantaci· n de las medidas de seguridad de nivel b§sico cuando: a) Los datos se utilicen con la ¼nica finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relaci· n con su finalidad. - Tambi®n podr§n implantarse las medidas de seguridad de nivel b§sico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaraci· n de la condici· n de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes p¼blicos.

4. Funciones y obligaciones de los usuarios

Los usuarios de atenci· n tienen las siguientes obligaciones:

CON RESPECTO A FICHEROS AUTOMATIZADOS

1. OBLIGACIONES GENERALES

1. Guardar el necesario secreto respecto a cualquier tipo de informaci· n de car§cter personal conocida en funci· n del trabajo desarrollado, incluso una vez concluida la relaci· n laboral con la organizaci· n.
2. Guardar todos los soportes f²sicos y/o documentos que contengan informaci· n con datos de car§cter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.
3. Queda prohibido el traslado de cualquier soporte, listado o documento con datos de car§cter personal en los que se almacene informaci· n titularidad de la organizaci· n fuera de los locales de la misma, sin autorizaci· n previa del Responsable de Seguridad. En el supuesto de existir traslado o distribuci· n de soportes y documentos se realizar§ cifrando dichos datos, o mediante otro mecanismo que impida el acceso o manipulaci· n de la informaci· n por terceros.
4. Ficheros de car§cter temporal o copias de documentos son aquellos en los que se almacenan datos de car§cter personal, generados para el cumplimiento de una necesidad determinada o trabajos temporales y auxiliares, siempre y cuando su existencia no sea superior a un mes. Estos ficheros de car§cter temporal o copias de documentos deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creaci· n y, mientras est®n vigentes, deber§n cumplir con los niveles de seguridad asignados por el Responsable de Seguridad.
Si, transcurrido el mes, el usuario necesita continuar utilizando la informaci· n almacenada en el fichero, deber§ comunicarlo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.
5.Ðnicamente las personas autorizadas en un listado de accesos podr§n introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protecci· n. Los permisos de acceso de los usuarios son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros o documentos a cuyo acceso no est§ autorizado, deber§ ponerlo en conocimiento del Responsable de Seguridad correspondiente.
6. Comunicar al Responsable de Seguridad, conforme al procedimiento de

notificaci· n, las incidencias de seguridad de las que tenga conocimiento.

2. OBLIGACIONES RESPECTO DE LOS FICHEROS AUTOMATIZADOS

1. Cambiar las contrase¶as a petici· n del sistema.
2. Cerrar o bloquear todas las sesiones al t®rmino de la jornada laboral o en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.
3. No copiar la informaci· n contenida en los ficheros en los que se almacenen datos de car§cter personal al ordenador personal, disquetes, port§til o a cualquier otro soporte sin autorizaci· n expresa del Responsable de Seguridad correspondiente.
4. Guardar todos los ficheros con datos de car§cter personal en la carpeta indicada por el Responsable de Seguridad correspondiente, a fin de facilitar la aplicaci· n de las medidas de seguridad que les correspondan.
5. Los usuarios tiene prohibido el env²o de informaci· n de car§cter personal de nivel alto, salvo autorizaci· n expresa del Responsable de Seguridad que tenga asignada esta tarea. En todo caso, este env²o ¼nicamente podr§ realizarse si se adoptan los mecanismos necesarios para evitar que la informaci· n no sea inteligible ni manipulada por terceros.
6. Los usuarios no podr§n, salvo autorizaci· n expresa del Responsable de Seguridad que tenga asignada esta tarea, instalar cualquier tipo de programas inform§ticos o dispositivos ni en los servidores centrales ni en el ordenador empleado en el puesto de trabajo.

7.Queda prohibido:

a. Emplear identificadores y contrase¶as de otros usuarios para acceder al sistema.

b. Intentar modificar o acceder al registro de accesos habilitado por el Responsable de Seguridad competente.

c. Burlar las medidas de seguridad establecidas en el sistema inform§tico, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.

d. Enviar correos masivos (spam) empleando la direcci· n de correo electr· nico corporativa.

e. Y en general, el empleo de la red corporativa, sistemas inform§ticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organizaci· n, o bien para la realizaci· n de actos que pudieran ser considerados il²citos.

Estas obligaciones s· lo ser§n exigibles a los usuarios de ficheros automatizados, en tanto en cuanto la organizaci· n disponga los medios adecuados en cada caso.

Ficheros afectados
- CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO

CON RESPECTO A FICHEROS NO AUTOMATIZADOS

1. Guardar el necesario secreto respecto a cualquier tipo de informaci· n de car§cter personal conocida en funci· n del trabajo desarrollado, incluso una vez concluida la relaci· n laboral con la entidad.
2. Mantener debidamente custodiadas las llaves de acceso a la residencia, a sus despachos y a los armarios, archivadores u otros elementos que contenga ficheros no automatizados con datos de car§cter personal, debiendo poner en conocimiento del Responsable de Seguridad cualquier hecho que pueda haber comprometido esa custodia.
3. Cerrar con llave las puertas de los despachos al t®rmino de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicaci· n, a fin de evitar accesos no autorizados.
4. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificaci· n, las incidencias de seguridad de las que tenga conocimiento.
5. Queda prohibido el traslado de cualquier listado o documento an§logo con datos de car§cter personal en los que se almacene informaci· n titularidad de la entidad fuera de los locales de la misma.
6. Guardar todos los soportes f²sicos o documentos que contengan informaci· n con datos de car§cter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.
7. Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.
8. Únicamente las personas autorizadas para ello en el listado de accesos podr§n introducir, modificar o anular los datos contenidos en los ficheros objeto de protecci· n. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no est§ autorizado, deber§ ponerlo en conocimiento del Responsable de Seguridad.
9. Ficheros de car§cter temporal son aquellos en los que se almacenan datos de car§cter personal, generados para el cumplimiento de una necesidad determinada,

siempre y cuando su existencia no sea superior a un mes. Los ficheros de car§cter temporal deben ser destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creaci· n y, mientras est®n vigentes, deber§n contemplarse las medidas de seguridad contenidas en este documento.

Ficheros afectados
- CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO

CON RESPECTO A LAS OBLIGACIONES COMO USUARIO DE ATENCIÓN

1. Guardar el necesario secreto respecto a cualquier tipo de informaci· n de car§cter personal conocida en funci· n del trabajo desarrollado, incluso una vez concluida la relaci· n laboral con la organizaci· n.
2. Mantener en secreto sus claves de acceso al sistema, debiendo poner en conocimiento del Responsable de Seguridad cualquier hecho que pueda haber comprometido el secreto.
3. Las contrase¶as de acceso al sistema son personales e intransferibles, siendo el usuario el ¼nico responsable de las consecuencias que pudieran derivarse de su mal uso, divulgaci· n o p®rdida.
4. Cambiar las contraseñas a petición del sistema.
5. Cerrar o bloquear todas las sesiones al término de la jornada laboral.
6. Bloquear las sesiones en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.
7. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificaci· n, las incidencias de seguridad de las que tenga conocimiento.
8. No copiar la informaci· n contenida en los ficheros en los que se almacenen datos de car§cter personal al propio ordenador, disquetes o a cualquier otro soporte sin autorizaci· n expresa del Responsable de Seguridad. Queda igualmente prohibido el traslado de cualquier soporte en los que se almacene informaci· n titularidad de la compa¶²a fuera de los locales de la misma.
9. Guardar todos los ficheros con datos de car§cter personal en la carpeta indicada por el Responsable de Seguridad a fin de facilitar la aplicaci· n de las medidas de seguridad que les correspondan.
10. Guardar todos los soportes f²sicos que contengan informaci· n con datos de car§cter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.
11. Asegurarse de que no quedan documentos impresos que contengan datos

protegidos impresos en la bandeja de salida de la impresora.
12. Únicamente las personas autorizadas para ello en el listado de accesos podr§n introducir, modificar o anular los datos contenidos en los ficheros objeto de protecci· n. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no est§ autorizado, deber§ ponerlo en conocimiento del Responsable de Seguridad,
13. Ficheros de car§cter temporal son aquellos en los que se almacenan datos de car§cter personal, generados para el cumplimiento de una necesidad determinada, siempre y cuando su existencia no sea superior a un mes. Los ficheros de car§cter temporal deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creaci· n y, mientras est®n vigentes, deber§n ser almacenados en la carpeta designada por el Responsable de Seguridad.
Si, transcurrido el mes, el usuario necesita continuar utilizando la informaci· n almacenada en el fichero, deber§ comunicarlo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.
14. El correo electr· nico es considerado por la entidad como elemento fundamental para las comunicaciones entre la organizaci· n y el resto de agentes, p¼blicos o privados, que intervienen en las relaciones propias de la actividad desarrollada. Por ello, el correo electr· nico sea cual sea la direcci· n asignada, se configura como una herramienta de trabajo no exclusiva, colectiva y de libre acceso, asignadas a §reas o puestos de trabajo y no a personas. Queda prohibido el uso del mismo para fines no relacionados con las funciones laborales encomendadas. El empleo del nombre o apellidos de los trabajadores o funcionarios junto al dominio de la organizaci· n en las direcciones de correo no significa la asignaci· n por la organizaci· n de un correo personal, esto se realiza ¼nicamente por motivos organizativos internos de asignaci· n de §reas y puestos de trabajo. Los usuarios tienen prohibido el env²o de informaci· n de car§cter personal de nivel alto, salvo autorizaci· n expresa del Responsable de Seguridad. En todo caso, este env²o ¼nicamente podr§ realizarse si se adoptan los mecanismos necesarios para evitar que la informaci· n no sea inteligible ni manipulada por terceros.
15. Los usuarios no podr§n, salvo autorizaci· n expresa del Responsable de Seguridad, instalar cualquier tipo de programas inform§ticos o dispositivos ni en los servidores centrales ni en el ordenador personal empleado para el desarrollo de su trabajo.
16. Conocer la existencia de derechos de los interesados (derecho acceso, rectificaci· n, cancelaci· n y, en su caso, oposici· n), as² como su procedimiento de respuesta ante el ejercicio de uno de ellos.
17. Queda prohibido:

a. Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.
b. Intentar modificar o acceder al registro de accesos habilitado por el Responsable de Seguridad.
c. Burlar las medidas de seguridad establecidas en el sistema inform§tico, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.
d. Utilizar Internet para tareas que no est®n relacionadas directamente con las funciones asignadas al usuario. La organizaci· n regular§ las modalidades de acceso y las restricciones o limitaciones del mismo. Queda prohibida la descarga de software o ficheros de cualquier tipo desde Internet, sin consentimiento expreso de la organizaci· n, y ello aunque resulte de un acceso consentido por motivos de trabajo.
e. Introducir contenidos en la red corporativa y/o ordenador personal que no guarden relaci· n con la actividad y objetivos de la entidad.
f. Enviar correos masivos (spam) empleando la direcci· n de correo electr· nico corporativa.
g. Y en general, el empleo de la red corporativa, sistemas inform§ticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organizaci· n, o bien para la realizaci· n de actos que pudieran ser considerados il²citos.

Ficheros afectados
- CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO - CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO

5. Gestión de incidencias

Se entiende por incidencia cualquier anomal²a que afecte o pudiera afectar a la seguridad de los datos.

En caso de conocer alguna incidencia ocurrida, el usuario debe comunicarla al responsable de seguridad competente que adoptar§ las medidas oportunas.

Las incidencias pueden afectar tanto a ficheros automatizados como no automatizados.

Ejemplos de incidencias comunes que pudieran afectar a los datos personales contenidos en ficheros automatizados son las siguientes:

- Alteraci· n en los permisos, altas o bajas de usuarios.

- Olvido de contrase¶a.

- Bloqueo de cuenta por reiteraci· n de intentos de conexi· n fallidos.

- P®rdida de datos.

Por su parte algunos ejemplos de incidencias que pueden afectar a ficheros no automatizados son los siguientes:

- Robo o p®rdida de llaves de lugares o soportes en donde se almacenen dichos ficheros no automatizados.

- Desaparici· n de documentos o soportes que contengan datos personales.

No obstante dicha relaci· n no es taxativa y debe comunicar al responsable de seguridad cualquier incidencia que afecte a los datos de car§cter personal.

El concreto procedimiento/s de gesti· n de incidencias implantado/s en la organizaci· n es/son el siguiente/s:

5.1. Procedimiento para la gesti· n de incidencias relativas a ficheros automatizados

El procedimiento de notificaci· n y gesti· n de incidencias relativo a ficheros automatizados al que se refiere el presente documento consiste en:

La gesti· n de notificaci· n de incidencias se notificar§ a trav®s de un enlace de una cuenta de correo electr· nico (incidencias.lopd@ual.es) en la p§gina web de la comisi· n de Seguridad inform§tica.
Dicho correo ser§ gestionado por el personal competente que gestionar§ las incidencias y llevar§ un registro de las mismas.

Ficheros afectados
- CONSULTAS JURÓDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÓDICO

No obstante y sin perjuicio de que en el ¼ltimo apartado se designan el/los responsable/s de seguridad a quien ha de dirigirse, en concreto el responsable de seguridad designado para la gesti· n de incidencias para ficheros automatizados es:

Diego Pérez

5.2. Procedimiento para la gesti· n de incidencias relativas a ficheros no automatizados

El procedimiento de notificaci· n y gesti· n de incidencias relativo a ficheros no automatizados al que se refiere el presente documento consiste en:

La gesti· n de notificaci· n de incidencias se notificar§ a trav®s de un enlace de una cuenta de correo electr· nico (incidencias.lopd@ual.es) en la p§gina web de la comisi· n de Seguridad inform§tica.
Dicho correo ser§ gestionado por el personal competente que gestionar§ las incidencias y llevar§ un registro de las mismas.

Ficheros afectados

- CONSULTAS JURÕDICAS
- EXPEDIENTES LITIGIOS
- INFORMES GABINETE JURÕDICO

No obstante y sin perjuicio de que en el ¼ltimo apartado se designan el/los responsable/s de seguridad a quien ha de dirigirse, en concreto el responsable de seguridad designado para la gesti· n de incidencias para ficheros no automatizados es:

Carmen Alicia García

6. Ejercicio de derechos

6.1. Introducci· n

No basta con garantizar el derecho del titular de los datos a conocer de la existencia de un fichero o tratamiento. Este conocimiento no le atribuir²a, per se, ninguna posibilidad de actuaci· n material. Precisamente una de las novedades que introduce el derecho fundamental a la protecci· n de datos en el §mbito de los derechos de la personalidad, es el de proporcionar a su titular un haz de facultades que permiten una conducta activa, y no meramente reactiva, a su titular. Por tanto, es necesario proporcionar al titular de la informaci· n personal las posibilidades de actuaci· n de que dispone para un control material de sus datos.

La Ley contempla una serie de derechos que se desarrollaron en la Instrucci· n 1/1998 y el reglamento de desarrollo de la LOPD los ha clarificado definitivamente.

Para ello nos referiremos primero a una serie de disposiciones comunes a todos los derechos y posteriormente se analizar§ cada uno de los derechos.

6.2. Disposiciones comunes

6.2.1. Car§cter personal²simo (Art²culo 23 RDLOPD)

El art²culo 23 del RDLOPD dispone que los derechos son personal²simos y ser§n ejercidos por el afectado para lo cual deber§ acreditar su identidad.

Tales derechos se ejercitar§n:

a. Bien por el interesado, acreditando su identidad, como despu®s se indicar§.

b. Bien por el representante acreditando la representaci· n:
   - el representante legal en los supuestos de menores de edad o incapaces.
   - o el representante voluntario en cualquier caso

6.2.2. Acreditaci· n de la personalidad o representaci· n (Art²culo. 23 RDLOPD)

La acreditaci· n de la personalidad del interesado se debe realizar mediante copia de DNI o documento v§lido. Como puede ser por ejemplo el carn® de conducir. Tambi®n es posible que se acredite mediante firma electr· nica, caso de tratarse de un procedimiento de ejercicio de derechos en v²a telem§tica.

En el caso de representaci· n, seg¼n sea un supuesto de representaci· n legal o voluntaria, deber§ aportarse el documento que confiere la representaci· n.

No obstante, en el caso de las administraciones se puede sustituir esta forma de acreditar la condici· n de interesado o de representante mediante otros medios como puede ser la comparecencia.

6.2.3. Condiciones generales para el ejercicio de los derechos de acceso (Art²culo 24 RDLOPD)

El RDLOPD relaciona una serie de condiciones generales para el ejercicio de los derechos.

La primera de las reglas se refiere a que se trata de derechos independientes, es decir: que el ejercicio de ninguno de ellos ese requisito previo para el ejercicio de otro.

La segunda de ellas es la que exige que se conceda al interesado un medio sencillo y gratuito para el ejercicio de los derechos.

La tercera de las reglas es la relativa a que el ejercicio por el afectado de sus derechos no podr§ suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan. Se concretan una serie de medios que no son v§lidos: cartas certificadas o semejantes, servicios de tarificaci· n adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

La ¼ltima de las reglas mencionadas se refiere a que deber§ atenderse la solicitud a¼n cuando el mismo no hubiese utilizado el procedimiento establecido espec²ficamente al efecto por aqu®l, siempre que el interesado haya utilizado un medio que permita acreditar el env²o y la recepci· n de la solicitud, y que ®sta contenga los elementos que despu®s se analizan.

6.2.4. Inicio: solicitud

El inicio del procedimiento de ejercicio de derechos se inicia con una solicitud. Dicha solicitud deber§ incluir una serie de elementos esenciales que son:

Å Nombre y apellidos del interesado y documento que acredite la personalidad o representaci· n.

Å Petici· n en que se concreta la solicitud.

Å Direcci· n a efectos de notificaciones, fecha y firma del solicitante.

Å Documentos acreditativos de la petici· n que formula, en su caso.

6.2.5. Contestaci· n

Esta solicitud deber§ ser contestada en plazo, tal y como se indica posteriormente.

El RDLOPD aclara ciertos aspectos relativos a la contestaci· n:

1. El primero se refiere a que el responsable deber§ contestar la solicitud con independencia de que figuren o no datos personales del afectado en sus ficheros.
2. El segundo a que si la solicitud no re¼ne todos los requisitos deber§ solicitarse la subsanaci· n de los mismos.
3. Y por ultimo una cuesti· n importante: se aclara que corresponde al responsable la prueba del cumplimiento del deber de respuesta, debiendo conservar la acreditaci· n del cumplimiento del mencionado deber.

6.2.6. Ejercicio de derechos ante el encargado del tratamiento

El art²culo 26 del RDLOPD establece un r®gimen para la tramitaci· n de las solicitudes que se presenten ante el encargado.

Se dispone una regla general que consiste en que cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deber§ dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva.

Y una excepci· n, que se refiere a que ello es as² a menos que en la relaci· n existente con el responsable del tratamiento se prevea precisamente que el encargado atender§, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificaci· n, cancelaci· n u oposici· n.

6.3. Derecho de acceso

6.3.1. Concepto (Art²culo 27 RDLOPD)

1. El derecho de acceso es el derecho del afectado a obtener informaci· n sobre si sus propios datos de car§cter personal est§n siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se est® realizando, as² como la informaci· n disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.
2. En virtud del derecho de acceso el afectado podr§ obtener del responsable del tratamiento informaci· n relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento. No obstante, cuando razones de especial complejidad lo justifiquen, el

responsable del fichero podr§ solicitar del afectado la especificaci· n de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deber§ facilitarle una relaci· n de todos ellos.

3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de R®gimen Jur²dico de las Administraciones P¼blicas y del Procedimiento Administrativo Com¼n.

6.3.2. Forma de acceso (Art²culo 28 RDLOPD)

1. Al ejercitar el derecho de acceso, el afectado podr§ optar por recibir la informaci· n a trav®s de uno o varios de los siguientes sistemas de consulta del fichero:

   a. Visualizaci· n en pantalla.

   b. Escrito, copia o fotocopia remitida por correo, certificado o no.

   c. Telecopia.

   d. Correo electr· nico u otros sistemas de comunicaciones electr· nicas.

   e. Cualquier otro sistema que sea adecuado a la configuraci· n o implantaci· n material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podr§n restringirse en funci· n de la configuraci· n o implantaci· n material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicaci· n escrita si ®ste as² lo exige.

3. El responsable del fichero deber§ cumplir, al facilitar el acceso, lo establecido en el T²tulo VIII del Reglamento.
   Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aqu®l no responder§ por los posibles riesgos que para la seguridad de la informaci· n pudieran derivarse de la elecci· n.
   Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a trav®s de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, ser§n de cuenta del afectado los gastos derivados de su elecci· n.

6.3.3. Contestaci· n

6.3.3.1. Otorgamiento del acceso (Artículo 29 RDLOPD)

1. El responsable del fichero resolver§ sobre la solicitud de acceso en el plazo m§ximo de un mes a contar desde la recepci· n de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petici· n de acceso, el interesado podr§ interponer la reclamaci· n prevista en el art²culo 18 de la Ley Org§nica 15/1999, de 13 de diciembre.
   En el caso de que no disponga de datos de car§cter personal de los afectados deber§ igualmente comunic§rselo en el mismo plazo.

2. Si la solicitud fuera estimada y el responsable no acompa¶ase a su comunicaci· n la informaci· n a la que se refiere el art²culo 27.1, el acceso se har§ efectivo durante los diez d²as siguientes a dicha comunicaci· n.

3. La informaci· n que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dar§ en forma legible e inteligible, sin utilizar claves o c· digos que requieran el uso de dispositivos mec§nicos espec²ficos.
   Dicha informaci· n comprender§ todos los datos de base del afectado, los resultantes de cualquier elaboraci· n o proceso inform§tico, as² como la informaci· n disponible sobre el origen de los datos, los cesionarios de los mismos y la especificaci· n de los concretos usos y finalidades para los que se almacenaron los datos.

6.3.3.2. Denegación del acceso. (Artículo 30 RDLOPD)

1. El responsable del fichero o tratamiento podr§ denegar el acceso a los datos de car§cter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un inter®s leg²timo al efecto.

2. Podr§ tambi®n denegarse el acceso en los supuestos en que as² lo prevea una Ley o una norma de derecho comunitario de aplicaci· n directa o cuando ®stas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informar§ al afectado de su derecho a recabar la tutela de la Agencia Espa¶ola de Protecci· n de Datos o, en su caso, de las autoridades de control de las comunidades aut· nomas, conforme a lo dispuesto en el art²culo 18 de la Ley Org§nica 15/1999, de 13 de diciembre.

6.4. Derechos de rectificaci· n y cancelaci· n

6.4.1. Concepto (Art²culo 31 RDLOPD)

1. El derecho de rectificaci· n es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2. El ejercicio del derecho de cancelaci· n dar§ lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.
   En los supuestos en que el interesado invoque el ejercicio del derecho de cancelaci· n para revocar el consentimiento previamente prestado, se estar§ a lo dispuesto en la Ley Org§nica 15/1999, de 13 de diciembre y en el RDLOPD.

6.4.2. Solicitud (Art²culo 32 RDLOPD. Ejercicio de los derechos de rectificaci· n y cancelaci· n)

La solicitud de rectificaci· n deber§ indicar a qu®datos se refiere y la correcci· n que haya de realizarse y deber§ ir acompa¶ada de la documentaci· n justificativa de lo solicitado.

En la solicitud de cancelaci· n, el interesado deber§ indicar a qu®datos se refiere, aportando al efecto la documentaci· n que lo justifique, en su caso.

6.4.3. Contestaci· n (Art²culo 32. Ejercicio de los derechos de rectificaci· n y Cancelaci· n)

El responsable del fichero resolver§ sobre la solicitud de rectificaci· n o cancelaci· n en el plazo m§ximo de diez d²as a contar desde la recepci· n de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petici· n, el interesado podr§ interponer la reclamaci· n prevista en el art²culo 18 de la Ley Org§nica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de car§cter personal del afectado deber§ igualmente comunic§rselo en el mismo plazo.

6.4.4. Comunicaci· n al cesionario (Art²culo 32. Ejercicio de los derechos de rectificaci· n y cancelaci· n)

Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deber§ comunicar la rectificaci· n o cancelaci· n efectuada al cesionario, en id®ntico plazo, para que ®ste, tambi®n en el plazo de diez d²as contados desde la recepci· n de dicha comunicaci· n, proceda, asimismo, a rectificar o cancelar los datos.

La rectificaci· n o cancelaci· n efectuada por el cesionario no requerir§ comunicaci· n alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Org§nica 15/1999, de 13 de diciembre.

6.4.5. Denegaci· n (Art²culo 33. Denegaci· n de los derechos de rectificaci· n y cancelaci· n)

1. La cancelaci· n no proceder§ cuando los datos de car§cter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

2. Podr§ tambi®n denegarse los derechos de rectificaci· n o cancelaci· n en los supuestos en que as² lo prevea una ley o una norma de derecho comunitario de aplicaci· n directa o cuando ®stas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informar§ al afectado de su derecho a recabar la tutela de la Agencia Espa¶ola de Protecci· n de Datos o, en su caso, de las autoridades de control de las Comunidades Aut· nomas, conforme a lo dispuesto en el art²culo 18 de la Ley Org§nica 15/1999, de 13 de diciembre.

6.5. Derecho de oposici· n

6.5.1. Concepto (Art²culo 34. Derecho de oposici· n)

El derecho de oposici· n es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de car§cter personal o se cese en el mismo en los siguientes supuestos:

a. Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo leg²timo y fundado, referido a su concreta situaci· n personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b. Cuando se trate de ficheros que tengan por finalidad la realizaci· n de actividades de publicidad y prospecci· n comercial, en los t®rminos previstos en el art²culo 51 del RDLOPD, cualquiera que sea la empresa responsable de su creaci· n.

c. Cuando el tratamiento tenga por finalidad la adopci· n de una decisi· n referida al afectado y basada ¼nicamente en un tratamiento automatizado de sus datos de car§cter personal, en los t®rminos previstos en el art²culo 36 de este reglamento.

6.5.2. Solicitud (Art²culo 35. Ejercicio del derecho de oposici· n)

El derecho de oposici· n se ejercitar§ mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposici· n se realice con base en la letra a) del art²culo anterior, en la solicitud deber§n hacerse constar los motivos fundados y leg²timos, relativos a una concreta situaci· n personal del afectado, que justifican el ejercicio de este derecho.

6.5.3. Contestaci· n (Art²culo 35. Ejercicio del derecho de oposici· n)

El responsable del fichero resolver§ sobre la solicitud de oposici· n en el plazo m§ximo de diez d²as a contar desde la recepci· n de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petici· n, el interesado podr§ interponer la reclamaci· n prevista en el art²culo 18 de la Ley Org§nica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de car§cter personal de los afectados deber§ igualmente comunic§rselo en el mismo plazo.

6.5.4. Exclusi· n (Art²culo 35. Ejercicio del derecho de oposici· n)

El responsable del fichero o tratamiento deber§ excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposici· n o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este art²culo.

6.6. Derecho de oposici· n a las decisiones basadas ¼nicamente en un tratamiento automatizado de datos

6.6.1. Concepto (Art²culo 36. Derecho de oposici· n a las decisiones basadas ¼nicamente en un tratamiento automatizado de datos)

Los interesados tienen derecho a no verse sometidos a una decisi· n con efectos jur²dicos sobre ellos o que les afecte de manera significativa, que se base ¼nicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, cr®dito, fiabilidad o conducta.

6.6.2. Excepciones (Art²culo 36. Derecho de oposici· n a las decisiones basadas ¼nicamente en un tratamiento automatizado de datos)

No obstante, los afectados podr§n verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisi· n:

a. Se haya adoptado en el marco de la celebraci· n o ejecuci· n de un contrato a petici· n del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o inter®s.
   En todo caso, el responsable del fichero deber§ informar previamente al afectado, de forma clara y precisa, de que se adoptar§n decisiones con las caracter²sticas se¶aladas en el apartado 1 y cancelar§ los datos en caso de que no llegue a celebrarse finalmente el contrato.

b. Est® autorizada por una norma con rango de Ley que establezca medidas que garanticen el inter®s leg²timo del interesado.

6.7. Procedimiento establecido por la organizaci· n

El procedimiento de gesti· n y resoluci· n de ejercicios de derecho consiste en:

1. Ante la consulta (por ejemplo llamada) sobre alg¼n ejercicio de derechos por parte de alg¼n interesado.: - Dar informaci· n sobre en qu® consiste el Derecho, plazos etc... Es decir sobre el procedimiento. - No ofrecerle datos sobre la persona, sobre el fondo del asunto etc. - Tomar nota (s· lo tomar nota) de la persona de que se trata (de su identidad) y del motivo. - Hacerle llegar (si lo pide) el impreso correspondiente para ejercitar el derecho por una v²a que permita dejar constancia (reporte de fax o copia email).
2. Ante la recepci· n de alguna petici· n de ejercicio de derechos (normalmente por carta, fax o email): - Si dispone del m· dulo de ejercicio de derechos de GESDATOS: introducir la solicitud en la herramienta. - Si no dispone del m· dulo de ejercicio de derechos de GESDATOS: remitir la solicitud inmediatamente al responsable de seguridad que tenga atribuida esta tarea.
3. Ante cualquier otra cuesti· n en esta materia.: - Acudir al responsable de seguridad que tenga atribuida esta tarea.

Ficheros afectados
- CONSULTAS JURÕDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÕDICO - CONSULTAS JURÕDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÕDICO

Documentación adicional

Adicionalmente a la informaci· n aqu² descrita, se encuentran disponibles los siguientes documentos ubicados en las siguientes URLs:

- http://cms.ual.es/UAL/universidad/otrosorganos/comisionseguridad/derechos/index.htm : Derechos de los Titulares de los Datos Personales

No obstante y sin perjuicio de que en el ¼ltimo apartado se designan el/los responsable/s de seguridad a quien ha de dirigirse, en concreto el responsable de seguridad designado para la gesti· n de incidencias para ficheros no automatizados es:

Mª Ángeles Piedra

7. Procedimiento para el uso del correo electrónico y en general de las TIC

La organizaci· n puede definir una pol²tica de uso y control del correo electr· nico, y tambi®n - en general - de uso y control de las TIC.

En caso de que la organizaci· n haya definido una pol²tica de uso y control del correo, o m§s gen®rica de las TIC, la misma debe ser conocida por los usuarios. Por ello - caso de haberse adoptado - se detalla a continuaci· n. Como usuario deber§ conocerla y cumplirla.

El procedimiento de uso y control del email y las TIC de la organizaci· n es el siguiente:

La normativa de uso del correo electr· nico se detalle en el documento del hiperv²nculo.

Ficheros afectados
- CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO

Documentación adicional

Adicionalmente a la informaci· n aqu² descrita, se encuentran disponibles los siguientes documentos ubicados en las siguientes URLs:

- http://cms.ual.es/idc/groups/public/@otros/@comisionseguridad/documents/documento/politica_seguridad_ual.pdf : Pol²tica de seguridad de la UAL. (aprobada el 2-may-2006)

8. Procedimiento para los envíos telemáticos

El RDLOPD, para los ficheros de nivel alto, obliga al cifrado de datos o la utilizaci· n de cualquier otro mecanismo que garantice que la informaci· n no sea inteligible ni manipulada por terceros, cuando los mismos vayan a ser objeto de transmisi· n a trav®s de redes p¼blicas o redes inal§mbricas.

En caso de que la organizaci· n haya definido un procedimiento para los env²os telem§ticos de nivel alto la misma se detalla a continuaci· n. Como usuario deber§ conocerla y cumplirla.

El procedimiento de env²os telem§ticos al que se refiere el presente documento consiste en:

El RDLOPD, para los ficheros de nivel alto, obliga al cifrado de datos o la utilizaci· n de cualquier otro mecanismo que garantice que la informaci· n no sea inteligible ni manipulada por terceros, cuando los mismos vayan a ser objeto de transmisi· n a trav®s de redes de telecomunicaciones.

El env²o de datos a trav®s de redes de telecomunicaciones supone la adopci· n de una serie de medidas organizativas y t®cnicas que se han de respetar y constituyen el procedimiento a seguir. Este procedimiento afecta a diversos niveles:

1) A nivel organizativo:
a) Los usuarios deben conocer (y as² se debe reflejar en su manual y/o en las normas usuario del sistema de informaci· n) las pautas a seguir al respecto.

b) El usuario deber§ contar con la autorizaci· n del Responsable del Fichero o del Responsable de Seguridad, que tenga atribuidas estas funciones por delegaci· n.

2) A nivel t®cnico, el Usuario, bien por su propia cuenta, mediante los mecanismos que se hubieran puesto a disposici· n o bien, por parte del Resposable de Seguridad y/o t®cnico inform§tico, debe proceder al cifrado de los datos o la utilizaci· n de cualquier otro mecanismo que garantice que la informaci· n no sea inteligible ni manipulada por terceros.

Los env²os telem§ticos de becas al Ministerio se realizan a trav®s de un Web Service, comprimido en Zip y encriptado con 64 bits.

Ficheros afectados
- CONSULTAS JURÕDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÕDICO

9. Procedimiento de registro de entrada de soportes

El RDLOPD obliga a la adopci· n de determinadas medidas para garantizar la seguridad de los datos que entran o salen de las organizaciones.

En el caso de entradas de soportes deber§ disponerse de un sistema de registro de entrada de soportes que contenga la informaci· n dispuesta reglamentariamente.

Tenga en cuenta que ellos es importante porque, especialmente las salidas de soportes y documentos, constituyen un hecho que puede ser cr²tico ya que en muchas ocasiones las mismas se realizan sin respetar las obligaciones tanto jur²dicas como t®cnicas dispuestas legalmente y suponen en ocasiones el acceso por parte de terceros a informaci· n que no deben conocer. Por tanto ante una entrada o salida de documentos o soportes que contengan ficheros con datos personales deber§ dirigirse al responsable de seguridad competente que le informar§ de la forma de proceder.

El procedimiento de entrada de soportes y documentos a los que se refiere el presente documento es el siguiente:

Las entradas de soportes que contengan datos personales, cuyo nivel de seguridad sea como m²nimo de nivel medio, deber§n ser registradas en el registro de GESDATOS que contiene la siguiente informaci· n: el tipo de documento o soporte, la fecha y hora, el emisor, el n¼mero de documentos o soportes incluidos en el env²o, el tipo de informaci· n que contienen, la forma de env²o y la persona responsable de la recepci· n que deber§ estar debidamente autorizada.

Ficheros afectados
- CONSULTAS JURÓDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÓDICO - CONSULTAS JURÓDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÓDICO

10. Procedimiento de registro de salida de soportes

El RDLOPD obliga a la adopci· n de determinadas medidas para garantizar la seguridad de los datos que entran o salen de las organizaciones.

En el caso de salidas de soportes deber§ disponerse de un sistema de registro de salida de soportes que contenga la informaci· n dispuesta reglamentariamente.

Adicionalmente las salidas de soportes deben estar autorizadas por el responsable de seguridad competente.

Tenga en cuenta que ellos es importante porque, especialmente las salidas de soportes y documentos, constituyen un hecho que puede ser cr²tico ya que en muchas ocasiones las mismas se realizan sin respetar las obligaciones tanto jur²dicas como t®cnicas dispuestas legalmente y suponen en ocasiones el acceso por parte de terceros a informaci· n que no deben conocer. Por tanto ante una entrada o salida de documentos o soportes que contengan ficheros con datos personales deber§ dirigirse al responsable de seguridad competente que le informar§ de la forma de proceder.

El procedimiento de salida de soportes y documentos a los que se refiere el presente documento es el siguiente:

Las salidas de soportes que contengan datos personales, como m²nimo de nivel medio, deber§n ser registradas en el registro de GESDATOS que contiene la siguiente informaci· n: el tipo de documento o soporte, la fecha y hora, el emisor, el n¼mero de documentos o soportes incluidos en el env²o, el tipo de informaci· n que contienen, la forma de env²o y la persona responsable de la entrega que deber§ estar debidamente autorizada.

Ficheros afectados
- CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO - CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO

11. Procedimiento de desechado y reutilización de soportes automatizados

El desechado y/o reutilizaci· n de soportes y documentos que contienen datos personales, tanto en ficheros automatizados como no automatizados, pueden suponer el acceso indebido por parte de terceros a los datos personales que se contienen en los mismos si no se realiza de forma correcta.

La organizaci· n debe de disponer de un procedimiento que detalle la forma de proceder en estos casos.

En el caso de soportes automatizados (medida a adoptar para TODOS LOS NIVELES) siempre que vaya a desecharse cualquier soporte automatizado que contenga datos de car§cter personal (cualquiera que sea su nivel) deber§ procederse a su destrucci· n o borrado, mediante la adopci· n de medidas dirigidas a evitar el acceso a la informaci· n contenida en el mismo o su recuperaci· n posterior. Tambi®n deber§ procederse al borrado de la documentaci· n cuando el soporte vaya a reutilizarse.

En caso de que la organizaci· n haya definido un procedimiento para el desechado o reutilizaci· n de soportes automatizados el mismo se detalla a continuaci· n. Como usuario deber§ conocerlo y cumplirlo.

El procedimiento de desechado o reutilizaci· n de soportes para ficheros automatizados consiste en:

El procedimiento de reutilizaci· n de soportes consiste en el formateado previo del dispositivo si ®ste lo permite, para su posterior reutilizaci· n.
En el caso de proceder a la destrucci· n del soporte (siempre que se procede a su destrucci· n es porque el soporte ha dado error), se proceder§ a su destrucci· n f²sica.

Ficheros afectados
- CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO

12. Procedimiento de desechado y reutilización de soportes no automatizados

El desechado y/o reutilizaci· n de soportes y documentos que contienen datos personales, tanto en ficheros automatizados como no automatizados, pueden suponer el acceso indebido por parte de terceros a los datos personales que se contienen en los mismos si no se realiza de forma correcta.

La organizaci· n debe de disponer de un procedimiento que detalle la forma de proceder en estos casos.

En el caso de soportes no automatizados (medida que se ci¶e al NIVEL ALTO, pero que se puede ampliar si as² se indica en el procedimiento a otros niveles) deber§ procederse a la destrucci· n de las copias o reproducciones desechadas de forma que se evite el acceso a la informaci· n contenida en las mismas o su recuperaci· n posterior.

En caso de que la organizaci· n haya definido un procedimiento para el desechado de soportes no automatizados el mismo se detalla a continuaci· n. Como usuario deber§ conocerlo y cumplirlo.

El procedimiento de desechado o reutilizaci· n de soportes para ficheros no automatizados consiste en:

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de car§cter personal deber§ procederse a su destrucci· n o borrado, mediante la adopci· n de medidas dirigidas a evitar el acceso a la informaci· n contenida en el mismo o su recuperaci· n posterior. Las medidas a aplicar ser§n:
En el caso de que se trate de documento en papel, cuando ®stos contengan datos de car§cter personal, queda prohibida su reutilizaci· n (a modo de papel reciclado). En todo caso, se proceder§ a su destrucci· n mediante el uso de la destructora de papel. Para la destrucci· n de un gran volumen de informaci· n se contratan los servicios de una empresa de destrucci· n confidencial.

Ficheros afectados
- CONSULTAS JURôDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURôDICO

13. Procedimiento de custodia de soportes no automatizados

El procedimiento de custodia de la organizaci· n es el siguiente:

Los dispositivos de almacenamiento de los documentos que contengan datos de car§cter personal disponen de mecanismos que obstaculizan su apertura. En el documento de seguridad se relaciona el mecanismo que obstaculiza la apertura en relaci· n con cada soporte.

Ficheros afectados
- CONSULTAS JURÕDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÕDICO

14. Procedimiento de archivo de ficheros no automatizados

El procedimiento de archivo es el siguiente:

El archivo de los soportes se realiza siguiendo un criterio funcional, seg¼n un cuadro de clasificaci· n, que permite su localizaci· n visual. Debido a su poco volumen no se dispone de un registro inform§tico de localizaci· n.

Debido al volumen de soportes existentes se dispone de un registro inform§tico que posibilita su localizaci· n.

Adicionalmente y debido al volumen de archivos, una vez los soportes han permanecido durante su vida ¼til en el archivo vivo pasan al archivo hist· rico.

Ficheros afectados
- CONSULTAS JURÕDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÕDICO

15. Procedimiento de restricción de acceso a ficheros no automatizados

El procedimiento de ubicaci· n de §reas restringidas de la organizaci· n es el siguiente:

Deber§n encontrarse en §reas en las que el acceso est® protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas §reas deber§n permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Ficheros afectados
- CONSULTAS JURÕDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÕDICO

16. Procedimiento de copia y reproducción de documentos

El RDLOPD dispone que en el caso de ficheros no automatizados que contengan datos de nivel alto las copias o reproducciones ¼nicamente podr§n ser realizadas bajo el control del personal autorizado en el documento de seguridad.

En caso de que la organizaci· n haya definido un procedimiento para la copia o reproducci· n de documentos el mismo se detalla a continuaci· n. Como usuario deber§ conocerlo y cumplirlo.

El procedimiento de copia y reproducci· n de documentos de la organizaci· n es el siguiente:

La generaci· n de copias o la reproducci· n de los documentos ¼nicamente podr§ ser realizada bajo el control del personal autorizado en el documento de seguridad. La reproducci· n de copias se realiza mediante petici· n formal escrita al personal competente en la materia (personal de archivo), seg¼n legislaci· n vigente en la materia.
Deber§ procederse a la destrucci· n de las copias o reproducciones desechadas de forma que se evite el acceso a la informaci· n contenida en las mismas o su recuperaci· n posterior.

Ficheros afectados
- CONSULTAS JURÕDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURÕDICO

17. Procedimiento de traslado de documentación

El RDLOPD obliga a adoptar ciertas medidas dirigidas a proteger la informaci· n contenida en ficheros no automatizados que sea objeto de traslado, cuando los mismos contengan informaci· n de nivel alto.

En caso de que la organizaci· n haya definido dichas medidas para proceder al traslado de documentaci· n de nivel alto (obligaci· n que podr§ ampliarse a cualquier otro nivel de datos si as² se indica) las mismas se detallan a continuaci· n. Como usuario deber§ conocerlas y cumplirlas.

El procedimiento de traslado de documentaci· n de la organizaci· n es el siguiente:

TRASLADO DE DOCUMENTACIč N PARA FICHEROS DE NIVEL ALTO
Siempre que se proceda al traslado de la documentaci· n contenida en un fichero deber§n adoptarse medidas dirigidas a impedir el acceso o manipulaci· n de la informaci· n objeto de traslado.

Ficheros afectados
- CONSULTAS JURĉDICAS - EXPEDIENTES LITIGIOS - INFORMES GABINETE JURĉDICO

18. Responsables de seguridad

El Responsable/s de seguridad es el encargado/s de autorizar, coordinar, controlar y en algunos casos ejecutar las medidas de seguridad dispuestas en materia de protecci· n de datos.

Tenga en cuenta que estas personas son muy importantes en el funcionamiento de un sistema de protecci· n de datos y que ante cualquier duda o cuesti· n en materia de protecci· n de datos deber§ de dirigirse a el/ellos. En el caso de que existan varios tenga en cuenta que tendr§n las tareas divididas.

Los responsables de seguridad designados por la organizaci· n son los siguientes:

Nombre y Apellidos	**Email**	**Departamento**
Carmen Alicia García		**Archivo y documentación**
Diego Pérez		**STIC**
Mª Ángeles Piedra		**Departamento jurídico**

ANEXO A. Modelo de notificación de incidencias del nivel básico

NOTIFICACIÓN DE INCIDENCIAS DEL NIVEL BÁSICO	
Nº de incidencia *(A ser rellenado por el Responsable de Seguridad o por el gestor del fichero concreto, en su caso)*	
Fecha de notificación	
Tipo de incidencia *(Anotar todos los detalles de interés de la incidencia)*	
Descripción detallada de la incidencia	
Fecha y hora en la que se produjo la incidencia	
Persona(s) que realiza(n) la notificación *(Especificar si son usuarios o no del Fichero)*	
Persona(s) a quien(es) se comunica	
Efectos que puede producir *(En caso de no subsanación o incluso independientemente de ella)*	

Firma de la Persona que realiza la comunicación

ANEXO B. Modelo de notificación de incidencias del nivel medio / alto

NOTIFICACIÓN DE INCIDENCIAS DEL NIVEL MEDIO / ALTO	
Nº de incidencia *(A ser rellenado por el Responsable de Seguridad o por el gestor del fichero concreto, en su caso)*	
Fecha de notificación	
Tipo de incidencia	
Descripción detallada de la incidencia	
Fecha y hora en la que se produjo la incidencia	
Persona(s) que realiza(n) la notificación *(Especificar si son usuarios o no del Fichero)*	
Persona(s) a quien(es) se comunica	
Efectos que puede producir *(En caso de no subsanación o incluso independientemente de ella)*	
Recuperación de datos *(A rellenar sólo si la incidencia es de este tipo)*	
Procedimiento realizado	
Datos restaurados	

NOTIFICACIÓN DE INCIDENCIAS DEL NIVEL MEDIO / ALTO	
Datos grabados manualmente	
Persona que ejecutó el proceso	
Autorización del Responsable de seguridad	
Firma de la Persona que realiza la comunicación	

ANEXO C. Modelo de derecho de acceso

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Universidad de Almería.con domicilio enSacramento, s/n de La Cañada de San Urbano. Almería

DATOS DEL INTERESADO

D./Dª. ____, mayor de edad, con domicilio en la C/ ____, nº _____, Localidad ________________________, Provincia ___________________, código postal ______, con D.N.I. ________________, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 15 de la Ley Orgánica 15/1999, y los artículos 25, 27 y 28 del Real Decreto 1720/2007.

SOLICITA.-

1.- Que se le facilite gratuitamente el acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso podrá interponerse la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos, artículo 18.1 de la Ley Orgánica 15/99 y artículo 30.3 del Real Decreto 1720/2007.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3.- Que esta información deberá ser proporcionada de forma legible e inteligible, previa trascripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron.

4. Que a efectos de notificaciones designo el domicilio arriba indicado.

En ________________________, a _____ de __________________ de _______,

Firmado:

NOTA:

1. Deberá presentarse mediante solicitud dirigida al Responsable del Fichero
2. Requisitos (Debe contenerse):
    1. Nombre y apellidos del interesado; fotocopia del DNI o pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento electrónico acreditativo de tal representación. La utilización de firma identificativa el afectado eximirá de la presentación de las fotocopias de DNI o documento equivalente.
    2. Petición en que se concreta la solicitud.
    3. Domicilio a efectos de notificaciones, fecha y firma del solicitante.
    4. Documentos acreditativos de la petición que se formula, en su caso.
3. Si desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

ANEXO D. Modelo de derecho de rectificación

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Universidad de Almería.con domicilio enSacramento, s/n de La Cañada de San Urbano. Almería

DATOS DEL INTERESADO

D./Dª. ____, mayor de edad, con domicilio en la C/ ____, nº _____, Localidad _________________________, Provincia ___________________, código postal ______, con D.N.I. ________________, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 25, 31 y 32 del Real Decreto 1720/2007.

SOLICITA.-

1. Que se proceda gratuitamente a la efectiva corrección en el plazo de diez días desde la recepción de esta solicitud, de los datos inexactos relativos a mi persona que se encuentren en sus ficheros.

2. Los datos a rectificar son los siguientes:

____

____

3. Los documentos que se acompañan a esta solicitud y que acreditan la veracidad de los datos a rectificar en caso de ser necesario, se relacionan a continuación y se adjuntan al presente escrito. Son los siguientes documentos:

Doc. nº 1
Doc. nº 2

4. Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.

5. Que, en el caso de que el responsable del fichero considere que la rectificación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer, de considerarlo conveniente, la reclamación prevista en el artículo 18.1. de la Ley 15/1999 y 33.3 del RD 1720/2007.

6. Que si los datos que deben ser rectificados hubiesen sido cedidos previamente, sea notificada al cesionario la rectificación practicada en el plazo de 10 días, a fin de que éste, a su vez, proceda a la rectificación de su fichero.

En ________________________, a _____ de __________________ de _______,

Firmado:

NOTA:

1. Deberá presentarse mediante solicitud dirigida al Responsable del Fichero
2. Requisitos (Debe contenerse):
    1. Nombre y apellidos del interesado; fotocopia del DNI o pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento electrónico acreditativo de tal representación. La utilización de firma identificativa el afectado eximirá de la presentación de las fotocopias de DNI o documento equivalente.
    2. Petición en que se concreta la solicitud: indicar el dato/s que sean erróneos y la correccción que debe realizarse.
    3. Domicilio a efectos de notificaciones, fecha y firma del solicitante.
    4. Documentos justificativos de la corrección solicitada.
3. Si desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

ANEXO E. Modelo de derecho de cancelación

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Universidad de Almería.con domicilio enSacramento, s/n de La Cañada de San Urbano. Almería

DATOS DEL INTERESADO

D./Dª. ____, mayor de edad, con domicilio en la C/ ____, nº _____, Localidad _________________________, Provincia ___________________, código postal ______, con D.N.I. ________________, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 25, 31 y 32 del Real Decreto 1720/2007.

SOLICITA.-

1. Que se proceda a la efectiva cancelación en el plazo de diez días desde la recepción de esta solicitud, de cualesquiera datos relativos a mi persona que se encuentren en su/s fichero/s mediante el borrado físico de los datos o, en su caso, el bloqueo con el fin de impedir su ulterior proceso o utilización.

2. Que me comuniquen por correo a la dirección arriba indicada la cancelación de los datos una vez realizada.

3. Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer, de considerarlo conveniente, la reclamación prevista en el artículo 18.1. de la Ley 15/1999 y 33.3 del RD 1720/2007.

4. Que si los datos que deben ser rectificados hubiesen sido cedidos previamente, sea notificada al cesionario la rectificación practicada en el plazo de 10 días, a fin de que éste, a su vez, proceda a la rectificación de su fichero.

En ________________________, a _____ de __________________ de _______,

Firmado:

NOTA:

1. Deberá presentarse mediante solicitud dirigida al Responsable del Fichero
2. Requisitos (Debe contenerse):
   1. Deberá indicarse si se revoca el consentimiento en los casos en que proceda.
   2. Nombre y apellidos del interesado; fotocopia del DNI o pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento electrónico acreditativo de tal representación. La utilización de firma identificativa el afectado eximirá de la presentación de las fotocopias de DNI o documento equivalente.
   3. Petición en que se concreta la solicitud.
   4. Domicilio a efectos de notificaciones, fecha y firma del solicitante.
   5. Documentos justificativos cuando se trate de la cancelación de un dato erróneo o inexacto.
3. Si desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

ANEXO F. Modelo de derecho de oposición

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Universidad de Almería.con domicilio enSacramento, s/n de La Cañada de San Urbano. Almería

DATOS DEL INTERESADO

D./Dª. ____, mayor de edad, con domicilio en la C/ ______________________________________, nº _____, Localidad ______________________, Provincia _________________, código postal ______, con D.N.I. _______________, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de oposición, de conformidad con los artículos 6.4, 17 y 30.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y los artículos 34 y 35 del RD 1720/2007 en consecuencia.

EXPONGO.-

1. La situación en que se produce el tratamiento y los motivos que suponen mi oposición al mismo son los siguientes (cuando proceda):

____

____

____

____

____

2. Para acreditar la situación descrita, acompaño una copia de los siguientes documentos (cuando proceda):

Doc. nº 1
Doc. nº 2

SOLICITO, que sea atendido mi ejercicio de derecho de oposición en los términos anteriormente expuestos. En el caso de que el responsable del fichero considere que dicha solicitud no procede o bien no sea atendida dentro del plazo establecido legalmente de diez días, esta parte podrá interponer, de considerarlo conveniente, la

reclamación prevista en el artículo 18.1. de la Ley 15/1999 y 35.2 del RD 1720/2007.

En _________________________, a _____ de ___________________ de _______,

Firmado:

NOTA:

1. Deberá presentarse mediante solicitud dirigida al Responsable del Fichero
2. Requisitos (Debe contenerse):
   1. Nombre y apellidos del interesado; fotocopia del DNI o pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento electrónico acreditativo de tal representación. La utilización de firma identificativa el afectado eximirá de la presentación de las fotocopias de DNI o documento equivalente.
   2. Petición en que se concreta la solicitud: indicar el tratamiento al que se opone y - en su caso - los motivos.
   3. Domicilio a efectos de notificaciones, fecha y firma del solicitante.
   4. Documentos justificativos de la oposición solicitada (cuando proceda).
3. Si desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

ANEXO G. Modelo de derecho de impugnación de valores

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Universidad de Almería.con domicilio enSacramento, s/n de La Cañada de San Urbano. Almería

DATOS DEL INTERESADO

D./Dª. ____, mayor de edad, con domicilio en la C/ ____, nº _____, Localidad _________________________, Provincia ___________________, código postal ______, con D.N.I. ________________, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de impugnación de valores, de conformidad con el artículo 13 de la Ley Orgánica 15/1999 y 36 del RD 1720/2007.

EXPONGO.-

(Que existe una decisión con efectos jurídicos que afecta de manera significativa, que se basa únicamente en un tratamiento automatizado de datos, destinada a evaluar determinados aspectos de mi personalidad. Es la siguiente:

____

____

____

____

____

SOLICITO, que sea atendido mi ejercicio de derecho de impugnación de valoraciones en los términos anteriormente expuestos y se me ofrezca información sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. En el caso de que el responsable del fichero considere que dicha solicitud no procede o bien no sea atendida dentro del plazo establecido legalmente de diez días, esta parte podrá interponer, de considerarlo conveniente, la reclamación prevista en el artículo 18.1. de la Ley 15/1999.

En ________________________, a _____ de __________________ de _______,

Firmado:

NOTA:

1. Deberá presentarse mediante solicitud dirigida al Responsable del Fichero
2. Requisitos (Debe contenerse):
   1. Nombre y apellidos del interesado; fotocopia del DNI o pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento electrónico acreditativo de tal representación. La utilización de firma identificativa el afectado eximirá de la presentación de las fotocopias de DNI o documento equivalente.
   2. Petición en que se concreta la solicitud: indicar el tratamiento al que se opone y - en su caso - los motivos.
   3. Domicilio a efectos de notificaciones, fecha y firma del solicitante.
3. Si desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

ANEXO H. Modelo de derecho de acceso (videovigilancia)

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Universidad de Almería.con domicilio enSacramento, s/n de La Cañada de San Urbano. Almería

DATOS DEL SOLICITANTE

D./Dª. ____, mayor de edad, con domicilio en la C/ _______________________________________, nº _____, Localidad ______________________, Provincia _________________, código postal _____, con D.N.I. _______________, del que acompaña fotocopia, así como una imagen [fotografía] actualizada, por medio del presente escrito manifiesta su deseo de ejercer su derecho deacceso, de conformidad con el artículo 15de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y el artículo 23 y ss del Real Decreto 1720/2007 por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Para el caso en que ostente la condición de representante legal o como representante voluntario de la persona de quien se pretende ejercitar el derecho, indique también su nombre, apellidos y adjunte fotocopia del DNI, así como documento/s que acredite/n tal condición:

Nombre y Apellidos:

____

DNI:

____

Por favor, a continuación, indique el lugar, fecha y hora aproximada en los que su imagen fue captada por el sistema de cámaras o videocámaras de Universidad de Almería.. A dichos efectos, se entenderá por hora aproximada la referida a una franja horaria inferior a sesenta minutos.

SOLICITA.-

1.- Que se facilite gratuitamente el acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, de modo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso,

podrá interponerse la oportuna reclamación ante la Agencia Española de Protección de Datos para iniciar el procedimiento de tutela de derechos, en virtud del artículo 18 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso. O bien, en el caso de poder efectuarse, por no afectar a derechos de terceros, la fecha y hora en la cual pueda acercarme a sus dependencias para la visualización de las imágenes.

3.- Que se facilite, en tanto no afecte a derecho de terceros, el acceso de modo inteligible a los datos [imágenes], que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En ________________________, a _____ de __________________ de _______,

Firmado:

ANEXO I. Modelo de derecho de cancelación (videovigilancia)

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Universidad de Almería.con domicilio enSacramento, s/n de La Cañada de San Urbano. Almería

DATOS DEL SOLICITANTE

D./Dª. ____, mayor de edad, con domicilio en la C/ ____, nº _____, Localidad _________________________, Provincia ___________________, código postal ______, con D.N.I. ________________, del que acompaña fotocopia, así como una imagen [fotografía] actualizada, por medio del presente escrito manifiesta su deseo de ejercer su derecho decancelación, de conformidad con el artículo 16de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y el artículo 23 y ss del Real Decreto 1720/2007 por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Para el caso en que ostente la condición de representante legal o como representante voluntario de la persona de quien se pretende ejercitar el derecho, indique también su nombre, apellidos y adjunte fotocopia del DNI, así como documento/s que acredite/n tal condición:

Nombre y Apellidos:____

DNI:____

Por favor, a continuación, indique el lugar, fecha y hora aproximada en los que su imagen fue captada por el sistema de cámaras o videocámaras de Universidad de Almería.. A dichos efectos, se entenderá por hora aproximada la referida a una franja horaria inferior a sesenta minutos.

SOLICITA.-

1.- Que se proceda a la efectiva supresión en el plazo de diez días desde la recepción de esta solicitud, de cualquier dato relativo a mi persona que se encuentre en sus ficheros al no existir vinculación jurídica o disposición legal que justifique su mantenimiento.

2.- Que se me comunique de forma escrita a la dirección arriba indicada la cancelación de los datos una vez realizada.

3.- Que, en el caso de que el Responsable del Fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer, de considerarlo conveniente, la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

En ________________________, a _____ de __________________ de _______,

Firmado: